UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/903,780	07/12/2001	John Border	PD-201020	1489

7590 08/18/2006

Hughes Electronics Corporation
Patent Docket Administration
P.O. Box 956
Bldg. 1, Mail Stop A109
El Segundo, CA 90245-0956

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 08/18/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/903,780	BORDER ET AL.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 June 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16,18,20 and 22-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16,18,20 and 22-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed on June 8, 2006. Claims 36-38 are newly added.

2. Claims 1-16, 18,20, and 22-38 are currently being considered.

Response to Arguments

3. Applicant's arguments filed June 8, 2006 have been fully considered but they are not persuasive for the following reasons:

Regarding claim 1, the Applicant argues that the Cited Prior Art (CPA), Gelman et al. (U.S. 6,415,329), does not teach tearing down the unspoofed connection based upon the identifying step. The Applicant states that there is no identifying step which leads to the termination of the tearing down of the unspoofed connection. This argument is not found persuasive. The CPA discloses "selectively changing the destination addressing information of incoming packets which are to be transmitted on the wireless link, to that of the gateway application's main socket, forcing the connection to be terminated" (column 10 lines 3-8). The emphasis should be put on the "selectively changing" and the fact that only the packets which are to be transmitted on the wireless link are spoofed. The identifying step is discussed by the CPA by stated "each GT gateway application 76 listens for incoming TCP connections on its main socket, which differs from the destination socket of packets traversing the wireless link" (column 9 line

66 – column 10 line 1). Therefore, the identifying step is performed by the gateway by listening for TCP packets which are going to traverse the wireless link.

Furthermore, the Applicant argues that motivation for using the secondary reference, Albert et al. (6,742,045), in combination with Gelman to teach a redundant platform for spoofing. This is not found persuasive. Gelman discusses limitations of the gateway, and states "a gateway may crash before all of the data has successfully reached the client" (column 14 lines 48-51). It is clear that Gelman viewed this crashing as a limitation of the reliability of TCP, and therefore, using the redundant platform disclosed by Albert would have been obvious for reasons stated in the previous Office action.

Regarding the newly added claims 36-38, the Applicant argues that the CPA does not teach "wherein the spoofed connection utilizes a protocol to alter the behavior of the spoofed connection by performing one of three-way handshake spoofing, local data acknowledgement, connection to backbone connection multiplexing, data compression, or prioritization of connections." This argument is not found persuasive. Gelman teaches a system comprising a client, a client gateway, a server, and a server gateway (column 16 lines 27-45). In the case of Gelman, instead of the server acknowledging the client, the client gateway acknowledges the client (local acknowledgement), but modifies the SYN packet so that the client thinks it is coming from the server (column 16 lines 39-45). Therefore, it is asserted that this spoofed connection utilizes local acknowledgements, and therefore, is taught by the CPA.

Therefore, the rejections for the pending claims is maintained as given below, and applied to the newly added claims 36-38.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-16,18,20, and 22-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gelman et al. (U.S. Patent No. 6,415,329) in view of Albert et al. (U.S. Patent No. 6,742,045).

Regarding claim 1, Gelman discloses:

A method for performing redundancy switching from a first platform to a second platform, the method comprising:

identifying a message received over an unspoofed connection according to a prescribed protocol as an unspoofed message (column 4 lines 10 –45, column 9 line 66 – column 10 line 8);

tearing down, during a predetermined period, the unspoofed connection based upon the identifying step (Figure 10, column 10 lines 1 – 8, column 15 line 47 – column 17 line 20).

Gelman does not explicitly disclose restarting a spoofed connection between the second platform and a host wherein the second platform serves as a redundant platform for the first platform, and the predetermined period is set to minimize delay for restarting of the spoofed connection. Albert teaches a system in which service managers have backup service managers for the purpose of providing a fail over scheme if a master service manager should fail (column 10 lines 41-51). The service managers may be implemented on a router, and provide a service for packets before forwarding the packets into the network (column 10 lines 24-30). Gelman also discloses apparatuses similar to service managers as the Performance Enhancing Proxies (PEPs) provide a service of changing the TCP packets in order to spoof a connection over a satellite link. Gelman does not explicitly disclose a scheme in the instance that the PEP should fail. Albert provides a failover scheme involving backup service managers that would continue to provide a specified service to the packets in the event that the main service manager should fail. This would provide relatively uninterrupted service to the endpoints, besides the startup time for the backup PEP to sync up, which would provide packets that could tolerate long delay links (e.g. satellite links). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have a redundant platform setup as in Albert to provide a backup PEP in the system of Gelman so that a backup can function as the primary did in the event that the primary should fail as to provide PEP service even if the primary PEP fails. Furthermore, the "operational status of service managers may be communicated on the service manager interface" (Albert: column 10 lines 45-46). The frequency of the updates is a

predetermined time set to minimize the down time of a service manager (PEP). Therefore, it is asserted that the predetermined time is the time between a service manager failing and an update being received, and it would have been obvious at the time of invention that this time is set so that there is a minimum down-time of service.

Regarding claim 8, Gelman discloses:

A communication system comprising:

a first platform configured to communicate with a remote platform (Figure 2, column 15 line 47 – column 17 line 20); and

a second platform configured to communicate with the remote platform, the second platform being configured to identify a message received from a local host over an unspoofed connection according to a prescribed protocol as an unspoofed message, wherein the second platform tears down, during a predetermined period, the unspoofed connection in response to the identified message to avoid delaying startup of a spoofed connection with the remote platform (Figure 2, Figure 10, column 4 lines 10 – 45, column 9 line 66 – column 10 line 8, column 15 line 47 – column 17 line 20).

Gelman does not explicitly disclose restarting a connection between the second platform and a host wherein the second platform serves as a redundant platform for the first platform. Albert teaches a system in which service managers have backup service managers for the purpose of providing a fail over scheme if a master service manager should fail (column 10 lines 41-51). The service managers may be implemented on a

router, and provide a service for packets before forwarding the packets into the network (column 10 lines 24-30). Gelman also discloses apparatuses similar to service managers as the Performance Enhancing Proxies (PEPs) provide a service of changing the TCP packets in order to spoof a connection over a satellite link. Gelman does not explicitly disclose a scheme in the instance that the PEP should fail. Albert provides a failover scheme involving backup service managers that would continue to provide a specified service to the packets in the event that the main service manager should fail. This would provide relatively uninterrupted service to the endpoints, besides the startup time for the backup PEP to sync up, which would provide packets that could tolerate long delay links (e.g. satellite links). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have a redundant platform setup as in Albert to provide a backup PEP in the system of Gelman so that a backup can function as the primary did in the event that the primary should fail as to provide PEP service even if the primary PEP fails.

Regarding claim 15, Gelman discloses:

A communication gateway for providing redundant communication in a communication system having a remote platform, the gateway comprising:

a communication interface configured to communicate with a primary gateway configured to support a spoofed connection over a backbone connection to the remote platform (Figure 10, column 10 lines 1 – 8, column 15 line 47 – column 17 line 20); and

a processor coupled to the communication interface and configured to restart a spoofed connection (Figure 2, Figure 10, column 4 lines 10 – 45, column 9 line 66 – column 10 line 8, column 15 line 47 – column 17 line 20).

Gelman does not explicitly disclose wherein the unspoofed messages are forwarded after a predetermined period to avoid delaying the restart of the spoofed connection. Albert teaches a system in which service managers have backup service managers for the purpose of providing a fail over scheme if a master service manager should fail (column 10 lines 41-51). The service managers may be implemented on a router, and provide a service for packets before forwarding the packets into the network (column 10 lines 24-30). Gelman also discloses apparatuses similar to service managers as the Performance Enhancing Proxies (PEPs) provide a service of changing the TCP packets in order to spoof a connection over a satellite link. Gelman does not explicitly disclose a scheme in the instance that the PEP should fail. Albert provides a failover scheme involving backup service managers that would continue to provide a specified service to the packets in the event that the main service manager should fail. This would provide relatively uninterrupted service to the endpoints, besides the startup time for the backup PEP to sync up, which would provide packets that could tolerate long delay links (e.g. satellite links). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have a redundant platform setup as in Albert to provide a backup PEP in the system of Gelman so that a backup can function as the primary did in the event that the primary should fail as to provide

PEP service even if the primary PEP fails. Furthermore, the "operational status of service managers may be communicated on the service manager interface" (Albert: column 10 lines 45-46). The frequency of the updates is a predetermined time set to minimize the down time of a service manager (PEP). Therefore, it is asserted that the predetermined time is the time between a service manager failing and an update being received, and it would have been obvious at the time of invention that this time is set so that there is a minimum down-time of service.

Regarding claim 22, Gelman discloses:

A communication gateway for providing redundant communication in a communication system having a remote platform, the gateway comprising:

means for identifying a message received over a connection according to a prescribed protocol as an unspoofed message (column 4 lines 10 –45, column 9 line 66 – column 10 line 8);

means for terminating, during a predetermined period, the connection based upon the identified message (Figure 10, column 10 lines 1 – 8, column 15 line 47 – column 17 line 20); and

means for restarting a spoofed connection (Figure 10, column 10 lines 1 – 8, column 15 line 47 – column 17 line 20).

Gelman does not explicitly disclose restarting a connection between the second platform and a host upon detection of a redundancy switch, wherein the second platform serves as a redundant platform for the first platform wherein the predetermined

period is set to minimize delay for restarting of the spoofed connection. Albert teaches a system in which service managers have backup service managers for the purpose of providing a fail over scheme if a master service manager should fail (column 10 lines 41-51). The service managers may be implemented on a router, and provide a service for packets before forwarding the packets into the network (column 10 lines 24-30). Gelman also discloses apparatuses similar to service managers as the Performance Enhancing Proxies (PEPs) provide a service of changing the TCP packets in order to spoof a connection over a satellite link. Gelman does not explicitly disclose a scheme in the instance that the PEP should fail. Albert provides a failover scheme involving backup service managers that would continue to provide a specified service to the packets in the event that the main service manager should fail. This would provide relatively uninterrupted service to the endpoints, besides the startup time for the backup PEP to sync up, which would provide packets that could tolerate long delay links (e.g. satellite links). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have a redundant platform setup as in Albert to provide a backup PEP in the system of Gelman so that a backup can function as the primary did in the event that the primary should fail as to provide PEP service even if the primary PEP fails. Furthermore, the "operational status of service managers may be communicated on the service manager interface" (Albert: column 10 lines 45-46). The frequency of the updates is a predetermined time set to minimize the down time of a service manager (PEP). Therefore, it is asserted that the predetermined time is the time between a service manager failing and an update being received, and it would

have been obvious at the time of invention that this time is set so that there is a minimum down-time of service.

Regarding claim 29, Gelman discloses:

A computer-readable medium carrying one or more sequences of one or more instructions for performing redundancy switching from a first platform to a second platform, the one or more sequences of one or more instructions including instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

identifying a message received over an unspoofed connection according to a prescribed protocol as an unspoofed message (column 4 lines 10 –45, column 9 line 66 – column 10 line 8); and

tearing down, during a predetermined period, the unspoofed connection based upon the identifying step (Figure 10, column 10 lines 1 – 8, column 15 line 47 – column 17 line 20).

Gelman does not explicitly disclose restarting a spoofed connection between the second platform and a host wherein the second platform serves as a redundant platform for the first platform and the predetermined period is set to minimize delay for restarting of the spoofed connection. Albert teaches a system in which service managers have backup service managers for the purpose of providing a fail over scheme if a master service manager should fail (column 10 lines 41-51). The service managers may be implemented on a router, and provide a service for packets before forwarding the

packets into the network (column 10 lines 24-30). Gelman also discloses apparatuses similar to service managers as the Performance Enhancing Proxies (PEPs) provide a service of changing the TCP packets in order to spoof a connection over a satellite link. Gelman does not explicitly disclose a scheme in the instance that the PEP should fail. Albert provides a failover scheme involving backup service managers that would continue to provide a specified service to the packets in the event that the main service manager should fail. This would provide relatively uninterrupted service to the endpoints, besides the startup time for the backup PEP to sync up, which would provide packets that could tolerate long delay links (e.g. satellite links). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have a redundant platform setup as in Albert to provide a backup PEP in the system of Gelman so that a backup can function as the primary did in the event that the primary should fail as to provide PEP service even if the primary PEP fails. Furthermore, the "operational status of service managers may be communicated on the service manager interface" (Albert: column 10 lines 45-46). The frequency of the updates is a predetermined time set to minimize the down time of a service manager (PEP). Therefore, it is asserted that the predetermined time is the time between a service manager failing and an update being received, and it would have been obvious at the time of invention that this time is set so that there is a minimum down-time of service.

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Gelman discloses:

The method according to claim 1, further comprising:

invoking a reset function, wherein the reset function transmits a reset message to a local host that forwarded the message to tear down the unspoofed connection (column 10 lines 1 – 9, column 22 lines 25 – 40, column 23 lines 25 – 34).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Gelman discloses:

The method according to claim 1, further comprising: determining whether the predetermined period has expired (column 5 lines 10 – 22, column 10 lines 1 – 38); and

forwarding unspoofed messages to a remote platform based upon the determining step (column 10 lines 1 – 38).

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Gelman discloses:

The method according to claim 1, wherein the prescribed protocol is the Transmission Control Protocol, the method further comprising:

determining whether global TCP spoofing is enabled (column 9 line 16 – column 10 line 37); and

selectively forward TCP segments unspoofed to a remote platform (column 9 line 16 – column 10 line 37).

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Gelman discloses:

The method according to claim 1, further comprising:

establishing a backbone connection from the second platform to a remote platform (Figure 10, column 15 line 47 – column 17 line 20); and

forwarding a spoofed message over the backbone connection to a remote host (Figure 10, column 15 line 47 – column 17 line 20).

Claim 7 is rejected as applied above in rejecting claim 1. Furthermore, Gelman discloses:

The method according to claim 1, further comprising: forwarding messages associated with another protocol to a remote platform irrespective of the predetermined period (column 9 line 65 – column 10 line 38).

Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, Gelman discloses:

The method according to claim 5, wherein the backbone connection in the establishing step includes a space link over a satellite network (Figures 1,2,14, column 1 line 21 – column 2 line 32).

Claim 36 is rejected as applied above in rejecting claim 5. Furthermore, Gelman discloses:

The method according to claim 5, wherein the spoofed connection utilizes a protocol to alter behavior of the spoofed connection by performing one of three-way handshake spoofing, local data acknowledgement, connection to backbone connection multiplexing, data compression, or prioritization of connections (column 16 lines 27-45), wherein the client gateway acknowledges the client instead of the server.

Claim 37 is rejected as applied above in rejecting claim 12. Furthermore, Gelman discloses:

The method according to claim 5, wherein the spoofed connection utilizes a protocol to alter behavior of the spoofed connection by performing one of three-way handshake spoofing, local data acknowledgement, connection to backbone connection multiplexing, data compression, or prioritization of connections (column 16 lines 27-45), wherein the client gateway acknowledges the client instead of the server.

Claim 37 is rejected as applied above in rejecting claim 26. Furthermore, Gelman discloses:

The method according to claim 26, wherein the spoofed connection utilizes a protocol to alter behavior of the spoofed connection by performing one of three-way handshake spoofing, local data acknowledgement, connection to backbone connection multiplexing, data compression, or prioritization of connections (column 16 lines 27-45), wherein the client gateway acknowledges the client instead of the server.

5. Claims 9-14 are system claims analogous to the method claims rejected above, and therefore, are rejected following the same reasoning.

6. Claims 16 and 18, and 20 are apparatus claims analogous to the method claims rejected above, and therefore, are rejected following the same reasoning.

7. Claims 23 – 28 are apparatus claims analogous to the method claims rejected above, and therefore, are rejected following the same reasoning.

8. Claims 30 – 35 are computer-readable medium claims analogous to the method claims rejected above, and therefore, are rejected following the same reasoning.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KA
08/11/2006

CHRISTOPHER REVAK
PRIMARY EXAMINER

8/15/06